REMARKS/ARGUMENTS

The Office Action of February 27, 2009, has been reviewed and carefully considered.

Reconsideration of the above-identified application, as herein amended, is respectfully requested.

Status of the application.

Claims 1, 2, 4-6, and 9-21, with claims 1 and 15 being independent, remain pending in this application. By this amendment, claims 1, 4-6, 9-11, and 15 are amended and claims 3, 7, and 8 are cancelled without prejudice or disclaimer.

In the Office Action of February 27, 2009, the drawings were objected to; claims 1-23 were rejected under 35 USC §112, second paragraph; Claims 1-5, 7-10, and 20 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,815,665 ("Teper") in view of U.S. Patent Publication 2002/0103999 ("Camnisch"); claim 6 was rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch, and further in view of U.S. Patent No. 6,397,329 ("Aiello"); claims 11-13 and 21 were rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch, and further in view of U.S. Patent Publication No. 2001/0011351 ("Sako"); claim 14 was rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch and Sako, and further in view of U.S. Patent No. 7,234,059 ("Beaver"); claims 15 and 16 were rejected under 35 U.S.C. §103 as unpatentable over Teper; claims 17 and 18 were rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Sako; and claim 19 was rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Beaver.

Applicants after carefully considering the Examiner's rejections, together with the comments provided in support thereof, traverse these rejections and submit that the claims are patentably distinct over the applied references.

Amendments to the Drawings.

The drawings were objected to under 37 C.F.R. §1.84(p)(5) on the ground that they do not include reference numbers that correlate to the steps mentioned on pages 10-11 of the specification. Applicants have amended Fig. 2 to include such reference identifiers. Reconsideration and withdrawal of this objection are requested.

Claims 1-21 are Definite.

Claims 1-21 stand rejected under 35 U.S.C. §112, second paragraph as indefinite. Claims 1, 9, and 15 have been amended in consideration of the Examiner's remarks.

In claim 1, the word "fast" has been removed. Further, the word "means" recited in line 6 of claim 1 has been replaced with "an anonymous certificate associated to a public key". Support for this amendment can be found in the specification as filed at, at least, page 17 lines 20-24, page 20 lines 12-17, page 21 lines 23-25, and page 22 lines 2-5. In addition, the word "session" in claim 1 has been replaced with the term "authentication session" for enhanced clarity. Support for this amendment can be found at least on page 6, lines 18-20.

Claim 3 was rejected under 35 U.S.C. §112, second paragraph. Applicants have cancelled claim 3, rendering this rejection moot. The subject matter of claim 3 has been incorporated into independent claim 1 with amendments in consideration of the Examiner's comments. Support for these amendments can be found at least at page 15, lines 14-15 of the specification as filed.

Based on these amendments to the claims, the rejections under 35 U.S.C. §112, second paragraph are deemed to have been overcome.

The Present Disclosure.

Disclosed is a method for providing secure access to data processing resources and enabling a server to prove each action of a client.[1] A general objective of the invention is to offer an anonymous user authentication service and a fast and economical mechanism for maintaining session authentication. Despite user anonymity, users are responsible for their actions because resources accessed during a session can if necessary revoke user anonymity, for example in the event of a dispute.

The claimed method of accessing a service comprises the steps of identifying and registering a client, authenticating the client to an anonymous certification authority, authenticating the client by producing an anonymous signature, and opening and maintaining an anonymous authentication session with a server. For each session, the user provides a single, unique, anonymous signature based on an initialization token to the server. Selective contact is allowed between the server and the anonymous certification authority to revoke the anonymity of the client. The invention also provides a system for opening and maintaining an authentication session guaranteeing non-repudiation, wherein for each session, the user provides a unique anonymous signature to the server.

According to the disclosed method and the system configured to operate in accordance with the disclosed method, a user provides a server with a unique anonymous signature based on the initialization token to the server for each session. (Specification as filed, p. 24, ll. 19-26.). As described at page 11, lines 4-22 of the specification as filed, a series of tokens corresponding to the claimed anonymous signature are calculated, which enable the user to open and maintain

[1] These descriptive details are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations that are not claimed. Further, this is not intended to argue any interpretation of any claim term that is narrower than would be understood by one of ordinary skill in the art in the context of the specification and the claims as a whole.

the session. Thus, if there are two different sessions started by the same user, then each session -- whether or not they occur simultaneously -- cannot use the same anonymous signature and the fact that both sessions emanated from the same user cannot be determined from the respective anonymous signatures so long as the anonymity is maintained.

Claims 1 and 15, and their dependent claims, are patentable over the cited references.

Among the recitations of amended independent claim 1 not present in the cited references is "maintaining the anonymous authentication session with the aid of the series of tokens, thereby enabling the server to prove each of the actions of the client."

According to claim 1, maintaining the anonymous authentication session with the series of tokens enables the server to prove each of the actions of the client. Because the client calculates the tokens, the client cannot repudiate any of the actions of the server. Thus, the claimed method and system provide the server with the ability to prove each action of the client using the initialization token and the remainder of the series of tokens.

In contrast, Teper discloses a method in which a client 40 registers with a certification authority, disclosed as brokering site 60, to access a server 50. Client 40 authenticates itself to the server 50 by signing a pseudorandom challenge message which is assigned by the server 50 using a password. The server 50 forwards the signature to the certification authority 60 as a pass-through response, and the certification authority 60 checks the validity of the signature to finalize the authentication of the client 40. The certification authority then provides server 50 with the result of the authentication (verification) and the session information as shown in Fig. 3 of Teper.

In the Office Action, the Examiner acknowledges that Teper does not explicitly teach the limitation of "selectively allowing contact between the server and the anonymous certification authority to revoke the anonymity of the client using the signature provided in step iii", and cites

Camnisch for this disclosure. However, the cited combination in fact fails to disclose maintaining the anonymous authentication session between a client and a server with the aid of tokens, thereby enabling the server to prove each action of the client, as recited in claim 1.

The Examiner asserts that the step of maintaining is disclosed at col. 11, lines 10-12 of Teper. (See Office Action at page 8). Applicants disagree. The cited portion of Teper actually relates to the sending of an error message to user 40 if the certification authority 60 does not successfully authenticate user 40. The cited portion of Teper fails to provide any mention or teaching of maintaining the anonymous authentication session as explicitly recited in Applicants'claims.

According to claim 1, maintaining the anonymous authentication session with the series tokens enables the server to prove each of the actions of the client, so that the client cannot repudiate any of these actions. This functionality is absent in the cited prior art and, therefore, claim 1 is deemed to be allowable over the cited reference combination.

Applicant notes that even if Teper provided its server 50 with the ability to prove each action of a client 40, one skilled in the art would necessarily use the challenge and response mechanism that is already taught and used in Teper for each action. This challenge and response mechanism would require the use of more than one signature per authentication session; indeed, each challenge response would typically require a new signature. Thus, one skilled in the art would not be motivated to modify Teper to achieve the presently claimed method in which only one unique signature is required for each session.

Claim 15 has been amended to correspond to claim 1, and is deemed to be allowable for at least the same reasons as is claim 1 as discussed above.

Conclusion.

Because the cited prior art references, whether taken alone or in combination, fail to disclose the maintaining of an anonymous authentication session with the aid of a series of tokens, and a system for implementing this method, claims 1 and 15, and each of the dependent claims, is deemed to be in condition for immediate allowance.

It is believed that no additional fees or charges are required at this time in connection with the present application. However, if any such additional fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By /Lance J. Lieberman/
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: June 29, 2009